Proof-of-Work cryptocurrency mining: a statistical approach to fairness

Li, Sheng-Nan ; Yang, Zhao ; Tessone, Claudio J

DOI: https://doi.org/10.1109/icccworkshops49972.2020.9209934

Proof-of-Work cryptocurrency mining: a statistical approach to fairness

Sheng-Nan Li
UZH Blockchain Center,
URPP Social Networks
University of Zurich
CH-8050 Zurich, Switzerland
shengnan.li@uzh.ch

Zhao Yang
UZH Blockchain Center,
URPP Social Networks
University of Zurich
CH-8050 Zurich, Switzerland
zhao.yang@business.uzh.ch

Claudio J. Tessone
UZH Blockchain Center,
URPP Social Networks
University of Zurich
CH-8050 Zurich, Switzerland
claudio.tessone@uzh.ch

***Abstract*—In Proof-of-Work Blockchain-based systems, the ledger is kept consistent through some participants solving cryptopuzzles, usually referred to as *block mining*. Conventional wisdom asserts that the mining protocol is incentive-compatible. However, whether some strategic mining behaviors occur in practice or not, has been the subject of extensive debate. In this paper, we target this question by detecting anomalies in the statistics of consecutive blocks among several popular cryptocurrency systems. Firstly, we measure the inequality of mining revenue distribution in each system. Secondly, we propose a statistical method to identify the selfish mining (SM) behavior, a mining attack strategy posited by Eyal and Sirer in 2014. Our method is based on abnormal (statistically significant) high probability of continuously mining blocks. Finally, we extend our method to detect the mining cartels, in which miners secretly get together and share information about newly mined blocks. Our analysis will contribute to the research of fairness in cryptocurrency mining by providing evidence that the aforementioned strategic mining behaviors do take place in practice.**

***Index Terms*—cryptocurrency, anomaly detection, selfish mining, mining cartel**

I. Introduction

The central part of many cryptocurrency systems is a decentralized and public blockchain. The consistency of system's ledger is maintained by all participants solving hash puzzles, which is usually called "block mining". In order to solve the puzzles, attempts have to be made through brute force, and therefore, *a priori*, the probability of finding a solution is proportional to the number of tries per unit of time a miner is able to perform. Each miner will be rewarded by a nominal amount of cryptocurrency (designed in the supply policy of the protocol) if said miner is the first acknowledged one to find a valid block in the longest chain of the network. This kind of "Proof-of-Work"(PoW) consensus is employed in almost 90% of public blockchains [1]. This type of rewarding system provides an incentive for miners to contribute their resources to the system, and is essential to the crypocurrency's decentralized nature. According to this mechanism, the more mining power (resources) a miner invests, the better his chance to solve the puzzle first [2]. Thus, miners often join in mining pools to share their mining powers, and to increase the chances of finding blocks.

The PoW-based cryptocurrencies rely on the requirement that the majority of miners are honest, i.e. they follow the mining protocol. However, as shown in the Literature there exist multiple strategies that could attack a blockchain-based platform. For instance, the double-spending attack, the routing attack, and the block withholding attack.

- In a *double-spending attack* [3], a miner attempts to use the same assets more than once. Although this kind of attack has never happened against the largest cryptocurrencies, it has happened to the smaller ones, such as Bitcoin Gold.
- *The routing attack* can partition the network and delay its block propagation. Previous studies [4] showed that the routing attack is practically possible. According to their analysis, during 2015 and 2016, most of the Bitcoin nodes were hosted in a few Internet Service providers (ISPs). Indeed, 60% of all possible Bitcoin connections crossed 3 ISPs.
- In the *block withholding attack*. According to the protocol, When a miner finds a block she should submit it to the peer nodes unconditionally. However, miners could decide to not submit the block, or to postpone submitting it [5]. The former one, which is named as sabotage, has no direct benefit for the attacker but can harm the other miners; while the latter one, which is also known as selfish mining (SM), is more complex. Eyal and Sirer [6] proposed and described the SM strategy as follows: "...the selfish mining pool keeps its mined blocks private, secretly forking the blockchain and creating a private branch; when selfish miner reveals blocks from the private branch to the public, the honest miners will switch to the recently revealed block, abandoning the shorter public branch...". The details can be shown in Fig. 1. The miners in the P2P mining network can be divided into selfish miner(red node) and honest miner(green and black nodes). At t_1, a selfish miner mines a block(in red) after the normal blockchain of t_0, and he will secretly mine on the private branch. Then, if the selfish miner continuously finds the next block(t_{2A}), he might publish two blocks and gain rewards of two blocks; however, if a honest

miner also find a block(in green) in same height(t_{2B}), the selfish miner will immediately publish its secret block, and there will be a competition. In later t_3, if the selfish miners find the next block after its own block(t_{3A}), it is also a successful attack; if an honest miner find the next block after the selfish miner's block(t_{3B}), selfish miner enjoys the revenue of his one block; if an honest miner find the next block after the honest miner's block(t_{3C}), the selfish miner enjoys nothing and loses the revenue. Eyal and Sirer also claimed that the honest miners would be forced to waste their efforts on the shorter public branch; and if the disproportionate rewards of selfish miners encourage more honest miners to join the selfish mining pool, it may cause the increase in the pool size to majority and finally destroy the decentralization of cryptocurrency ecosystem.

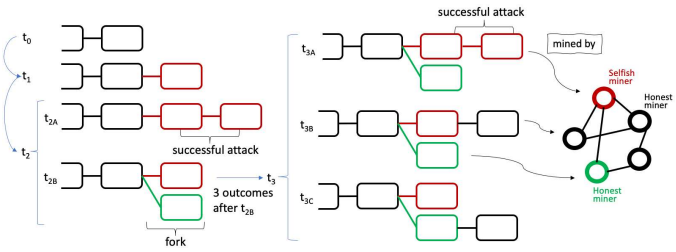

Fig. 1. Diagram of selfish mining strategy.

The discovery of SM attack has drawn a lot of attention and many extended mining strategies have been proposed, such as *stubborn mining* [7], and *publish-n strategy* [8]. These expended strategies lower down the profitable threshold of doing SM attack from 25% hash power [6], to 23.21% [9], or even 21.48% [10]. Meanwhile, scholars also propose various defenses strategies against these attacks. Existing defenses can be categorized into two approaches: 1) making fundamental changes to the block validity rules, for example *ZeroBlock* [11]: this is a timestamp-free solution which requires that each block must be generated and received by the network within a maximum acceptable time interval, and 2) lowering the chance of honest miners working on the selfish miner's chain during a forked situation, for example *weighted FRP* [12]: it asks miners to compare the weight of the chains instead of their length. However, selfish miners' timely reaction to another competitive block, and the high cost of changing the blockchain's fundamental rules, both bring difficulties to efficiently defense SM attack. In addition, there are still some debates on whether SM strategy could be profitable for selfish miners: some scholars argue that selfish miners can never earn extra revenue but only put themselves at risk for no gain [13]. These previous studies focus more on the influence of SM attack and the way to defend from it, mostly through building simulation or economic models on the cost-benefit analysis. However, there is little empirical evidence on whether miners do behave against the mining protocols in practice [14], which can bring more fundamental to the further researches about miners' strategic behavior. The question of whether selfish mining exists or not in practice is largely left unanswered so far.

In this paper, we try to answer this question through empirical analysis on the mining fairness among some popular PoW-based cryptocurrencies, including Bitcoin, Litecoin, Ethereum and Bitcoin Cash systems. Ignoring the controversial influence of SM strategy on the amount of miners' revenue, we sue the fact that selfish miners' behavior of selectively revealing their mined blocks would cause abnormal probability of consecutively mining blocks. Based on this insight, we propose an identification method of SM behavior by assessing miner's output of mining two blocks continuously. Furthermore, our method can be extended from single miner(mining pool) to pair of miners, and be used to identify the mining cartel. When secretly built a cartel, miners of the cartel will benefit from the huge mining power, as well as the information of blocks mined by the other members.

Our main contribution is threefold: First and foremost, up until this work, there was no definite conclusion about whether some miners are behaving against the protocol. To the best of our knowledge, our detection of the SM attack and mining cartel in crypotocurrency system is presented for the first time. In our Miner Sequence Bootstrapping model(MSB), we provide a robust statistical method to identify the most suspicious users conducting SM strategy. Secondly, most of the existing studies on the threshold of mining power are focusing on the individual mining pools, and ignoring the fact that several mining pools could secretly work together as mining cartels. Our paired MSB model is used to identify the secret mining cartels. Our results show that there are some abnormal mining pools that cannot be identified as selfish miners do participant in mining cartels. Finally, we highlight the importance of conducting empirical analyses when investigating the fairness of blockchain-based ecosystems: mathematical or economical models that focus on the cost-benefit analysis are not suitable enough, as participants of cryptocurrencies might have bounded rationality or be risk seeking.

II. Methods

A. Revenue Inequality Indexes

Gini index. The Gini index is the most frequently used inequality index of income or wealth distribution among a nation's residents [15], [16]. The Gini index can theoretically range from 0 (complete equality) to 1 (complete inequality), and is given by,

$$G = \frac{\sum_{i=1}^{N}\sum_{j=1}^{N} x_i - x_j}{2n\sum_{i=1}^{N} x_i} \tag{1}$$

where x_i is the wealth or income of an agent i, and there are N agents.

Theil index. The Theil index is an entropy-based measure that can be viewed as a measure of redundancy, lack of diversity, isolation, segregation, inequality, non-randomness,

and compressibility [17]. If the characteristic x_i is the income of N agents, the Theil *T* index is defined as:

$$T_T = \frac{1}{N}\sum_{i=1}^{N}\frac{x_i}{\mu}\ln\left(\frac{x_i}{\mu}\right) \tag{2}$$

If all agents have the same income, then the Theil *T* equals 0. If one agent owns all the income, then Theil *T* gives the result $\ln N$, which is maximum level of inequality attained by the measure Theil *T*. The Theil *L* index is defined as:

$$T_L = \frac{1}{N}\sum_{i=1}^{N}\ln\left(\frac{\mu}{x_i}\right) \tag{3}$$

where μ in these two indexes is the mean income:$\mu = \frac{1}{N}\sum_{i=1}^{N} x_i$

Both Theil *T* and Theil *L* are decomposable, and the difference between them is the part of the outcome distribution that each index is used for. Theil *L* index is more sensitive to the differences at the lower end of the distribution, while Theil *T* index is more sensitive to those at the top of the distribution.

Here we apply all these three indexes to the distribution of the monthly mining revenue among miners in each cryptocurrency. The x_i is the number of blocks a miner i has solved during a month, and there are N miners who have mined at least one block during this month.

B. Identification Method of Selfish Mining

According to the "PoW" protocol, the fair proportion of blocks a miner may discover during a time period (revenue share) is equal to his devoted mining power (number of attempts to solve the puzzle) divided over the total mining power of the network. In this idealized view, the discovery of each block is random and independent without influence from the previous blocks, since the information diffuses through the network instantaneously [18]. Thus, it is reasonable to assume that during a certain time period there exists an expected number of blocks that one miner can discover (which is proportional to the miner's mining power), while the order of miners who mined blocks in this period should be random. When doing strategic mining behavior (e.g. SM attack), however, the miners selectively publish their mined blocks. This should lead to an identifiable increase in their success rate of discovering two blocks consecutively (although it may not significantly increase either the amount or the proportion of blocks mined by selfish miners during that time period [13]).

In this study, we have proposed an identification method, named *Miner Sequence Bootstrapping model(MSB)*. It controls the amount of blocks mined by each miner during a period, and then repeatedly shuffles the sequence of miners' discoveries of these blocks. This model could provide the distribution and the expected number of times that each miner could continuously discover two blocks. In the t-th shuffle round, the number of times that miner i continuously mines two blocks during period T is denoted as $S_i^T(t)$. We have performed a bootstrap analysis of the mining output of each miner i by comparing the actual times C_i^T that miner i continuously discover two blocks in period T with the expected times $S_i^T(t)$ based on the shuffled simulation. The measurement of miner's mining behaviors be can be defined as:

$$MSB_i^T = \frac{C_i^T - \left\langle S_i^T \right\rangle}{\sigma\left[S_i^T\right]} \tag{4}$$

where $\left\langle S_i^T \right\rangle$ and $\sigma\left[S_i^T\right]$ are the expected value and the standard deviation of all the observations $S_i^T(t)$, respectively.

If $MSB_i^T > 0$, it means that for consecutively discovering two blocks during period T, miner i succeeded more times than he could (i.e. based on his revenue share). The larger the MSB_i^T index, the more abnormal behavior of miner i in period T. In order to identify abnormal miners with different levels in conducting SM strategy, we need to adjust the criterion of our identification model. In details, when we set the criterion as $MSB > 2$ (with a confidence of 95%), it means that any miner whose MSB index of a certain period exceeds 2 will be identified as a selfish miner by our model.

C. Identification Method of Mining Cartel

We would like to point out that the existence of mining cartels has been ignored in many previous studies. The conventional wisdom believes that the mining protocol is secure as long as the pool's mining power is limited in certain threshold. However, these assessments are based on the assumption that the mining pools are operating independently. In theory, mining pools could build secret cartels. The participants of these secret cartels would benefit from the huge mining power of the cartels, as well as the information of the mined blocks shared by the other members. Thus, we believe that the probability of continuous discovery of blocks among miners in the same cartel will be abnormal. Therefore, in this part, we would like to verify if mining pools have formed secret cartels by extending our identification method to pairs of mining pools, named as *paired Miner Sequence Bootstrapping model(paied MSB)*. When doing the identification of mining cartels, the measurement of anomalies in the properties of consecutive blocks' statistics between two miners, i and j, can be defined as:

$$MC_{ij}^T = \frac{C_{ij}^T - \left\langle S_{ij}^T \right\rangle}{\sigma\left[S_{ij}^T\right]} \tag{5}$$

where C_{ij}^T is the actual times that two consecutive blocks are first mined by miner i, then by miner j. S_{ij}^T is the observed value of each shuffle round that the number of times two consecutive blocks are first mined by miner i, then by j during period T. $\left\langle S_{ij}^T \right\rangle$ and $\sigma\left[S_{ij}^T\right]$ are the corresponding expected value and the standard deviation, respectively. After determining the criterion of the paired MSB model as $MC > 2$, we can label pairs of miners whose MC indexes are larger than 2 as mining cartels during certain period.

III. Description of Datasets

In this study, we have conducted statistical analysis on four "PoW"-based crytocurrencies, which are the Bitcoin, Litecoin, Ethereum and Bitcoin Cash.

- **Bitcoin.** Bitcoin was started on 3 Januaray 2009 when the internet persona Satoshi Nakamoto mined the genesis block. Nowadays, this most famous digital asset has a rich and extensive ecosystem with a total market capitalization over 140 billions of US Dollars. About every 10 minutes, a new block is created and quickly published to all nodes.
- **Litecoin.** Litecoin was a fork of the Bitcoin Core client. The Litecoin network went live on 13 October 2011 differing primarily by having a decreased block generation time (2.5 minutes), increased maximum number of coins, different hashing algorithm, and a slightly modified GUI.
- **Ethereum.** Ethereum was proposed in late 2013, and went live on 30 July 2015 featuring smart contract functionality. The block time of Ethereum is 14 to 15 seconds.
- **Bitcoin Cash.** Bitcoin Cash was a hard fork of Bitcoin that seeks to add more transaction capacity to the network. The first Bitcoin Cash software implementation was released on 1 August 2017. In both Bitcoin and Bitcoin Cash, one new block will be generated every ten minutes on average. Bitcoin Cash had an instability in mining difficulty around Octobor 2017, resulting in being thousands of blocks ahead of Bitcoin.

Our datasets of four crytocurrencies contain information of blocks from their launch to the end of 2019, including block height, mined time, the corresponding miners, etc.

IV. Results

A. Evolution of miners and blocks

From the genesis block to the one at the end of 2019, the number of blocks and mining pools during each month in each cryptocurrency system are shown in Fig. 2. One can find that the mining markets of all the four cryptocurrencies have unstable stages with different lengths after launch. To minimize the error in our following identification of strategic mining behaviors, our simulation experiment only focuses on the relative stable periods for both miners and blocks. That is split by the dash line in Fig. 2), which marks out the beginning of our simulation time-window in each cryptocurrency: January 2012 in Bitcoin, May 2015 in Litecoin, September 2015 in Ethereum, and December 2017 in Bitcoin Cash.

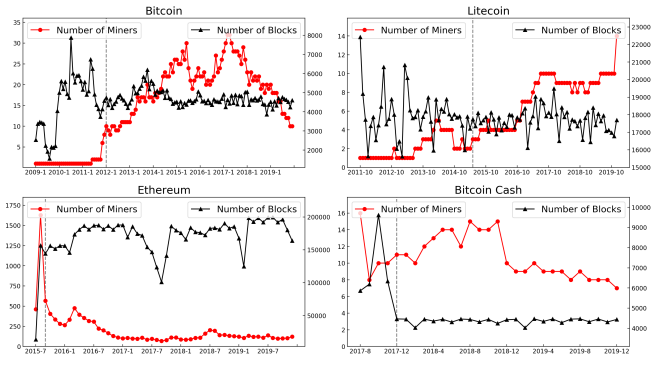

Fig. 2. Monthly number of miners and blocks in Bitcoin, Litecoin, Ethereum, Bitcoin Cash

B. Revenue share among large pools

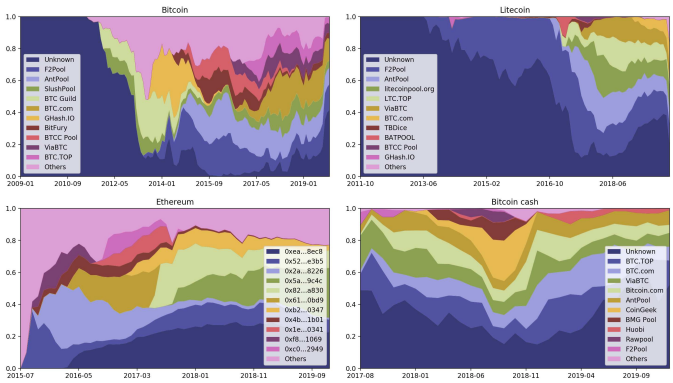

Fig. 3. Monthly revenue share among miners in Bitcoin, Litecoin, Ethereum, Bitcoin cash

We have shown the monthly revenue distributions of some large mining pools in Fig. 3. The "Unknown" miner are some mining addresses whose identities cannot be traced back to any known entity. It is worth to mention that some of the unknown mining addresses might be owned by named pools (e.g. to hide their activities such as selfish mining). In our Ethereum dataset, each block was mined by a known hash address, while "Unknown" mining addresses exist in all the other three cryptocurrencies. In detail, one can observe that in Bitcoin and Litecoin more and more rewards were gained by named pools, and in Bitcoin Cash there are more than 20% of blocks are mined by "Unknown" miners all the time. According to the "PoW" mechanism, the revenue share can reflect these pools' mining power in some extent. Therefore, these four cryptocurrency systems seem to be secure when only assess on the statistic result of revenue share: There are few miners sometimes hold more than 25% of the total power, and no one holds a mining power in excess of the majority(50%).

C. Inequality of mining revenue distribution

To further study the fairness of mining in each cryptocurrency system, we measured the inequality among values of mining revenue distribution using *Gini* index, *Theil-T* index, and *Theil-l* index. The inequality of miners' monthly revenue are shown in Fig. 4, in which the result of Ethereum is based on all its miners, while results of the other three cryptocurrencies are based on their named mining pools. According to these three inequality indexes, the mining revenue among all miners in Ethereum is very unequal: most of the blocks are mined by a very small group of miners, and its Gini indexes of each month are always above 0.9. In addition, when focusing more on the revenue among small pools(from *Theil-l* index) than that among large pools(from *Theil-T* index), all the four cryptocurrencies present a higher inequality in terms of mining revenue. The larger *Theil-l* indexes also indicate that there are seemingly many pools with very low mining power in each system when not considering the potentially secret associations among them.

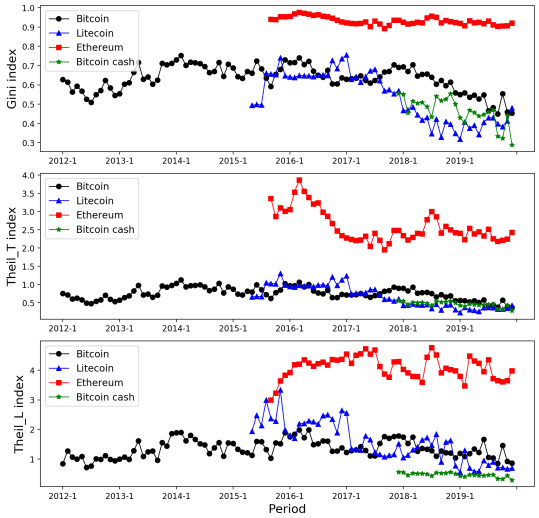

Fig. 4. Three inequality indexes of monthly mining revenue in Bitcoin, Litecoin, Ethereum, Bitcoin Cash

D. The MSB indexes of miners

In the main part of this study, we have proposed a MSB model to identify the most suspicious selfish miners in cryptocurrency systems. We have focused on the period when the number of blocks and miners were relatively stable, and then conducted 1000 times shuffle simulations on the block mining outputs of each month. The pools' monthly MSB indexes calculated by our MSB model corresponding to their revenue share are shown in Fig. 5. As we have mentioned before, according to the "PoW" protocol, one miner's revenue share during a period can reflects his mining power of this period. Therefore, the results in Fig. 5 show that in Bitcoin, Litecoin and Ethereum, some miners with less mining powers might conduct more SM strategy, while in Bitcoin Cash mining, pools with various mining powers could involve in SM strategy.

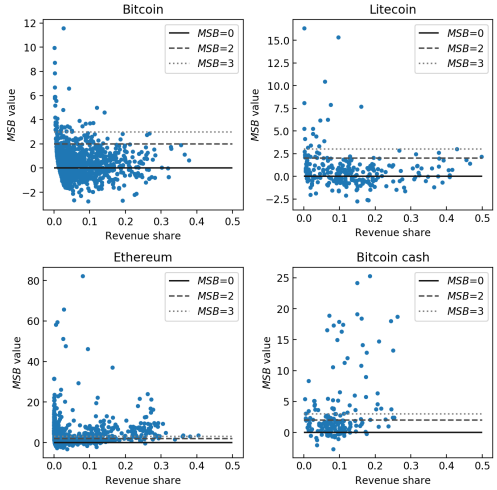

Fig. 5. Monthly MSB index of miners corresponding with their monthly revenue share in Bitcoin, Litecoin, Ethereum, Bitcoin Cash

E. Identified selfish miner

Under the criterion $MSB > 2$, which means that any miner i whose MSB_i^T index of month T exceeds 2 will be identified as a selfish miner by our MSB model. These detected selfish miners in every cryptocurrency are shown in Fig. 6, where the miners are ranked by the number of times they have been identified (we have only displayed the top 8 miners in each cryptocurrency). The identification results show that the SM strategy might have been implemented by several miners in each system, and the identified selfish miners in Ethereum and Bitcoin Cash might be more likely to continuously behave in SM strategy.

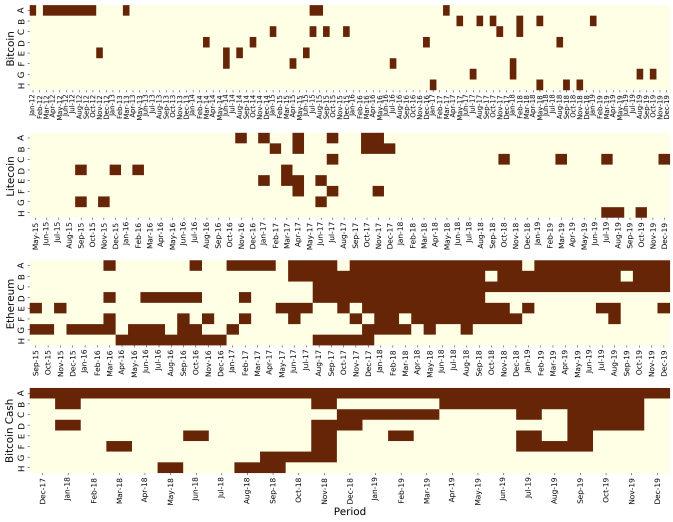

Fig. 6. The identified selfish miners of each month in Bitcoin, Litecoin, Ethereum, Bitcoin Cash

F. Identified mining cartel

To detect the existence of mining cartel, we used the paired MSB model to calculate the monthly MC value of each pair of miner pools (in Ethereum, because of the enormous amount of miners, we could only include pools with more than 1% revenue share). After determining the criterion of the paired MSB model as $MC > 2$, we have labeled pairs of miners $i - j$ whose MC_{ij}^T values of month T are larger than 2 as mining cartels. The number of times that each pair of miners is labeled as a mining cartel are shown in Fig. 7. The miners are ranked by the sum of times they have been identified as a member in a cartel. We show the mining cartels among the top 20 miners in Bitcoin and Ethereum, and among all the miners in Litecoin and Bitcoin Cash. We have noticed that some abnormal mining pools that can not be identified by our first model do participant in cartels. Besides, mining cartel is more common among different miners in Bitcoin system, but less common in Ethereum. In Litecoin and Bitcoin Cash, mining cartel is always built by certain group of miners.

V. Discussion

Given the fact that for blockchain-based systems, prior trust between users is not a requirement [19], [20], enabling fairness

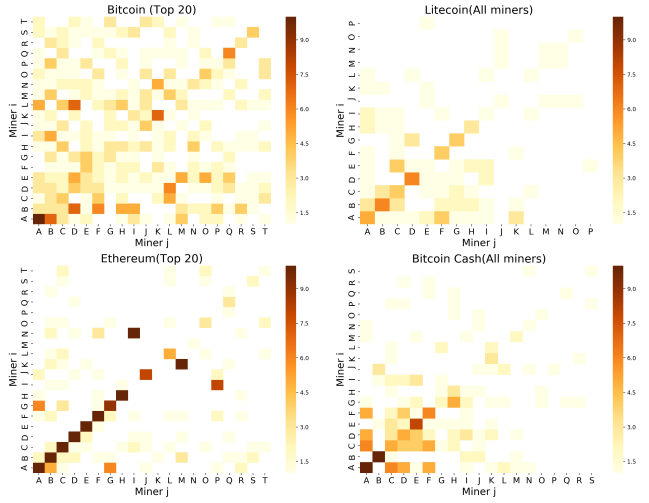

Fig. 7. Frequency of building cartel among different mining pools in Bitcoin, Litecoin, Ethereum, Bitcoin Cash

at all the levels in cryptocurrencies system is mandatory. In this paper, we have developed a new methodology and conducted statistical analysis on mining fairness in four "PoW"-based crytocurrencies.

In the first study, we have shown the evolution on number of miners and blocks, and we also find that the revenue distribution among all miners in Ethereum is unequal. By proposing a Miner Sequence Bootstrapping(MSB) model, we are able to identify abnormal miners, in the sens the likelihood to mine consecutive blocks in a system is much larger than that of a fair distribution (given the realised share of nodes they mine). We believe that the reason why some mining pools could have abnormal continuously success rates is because they are employing the selfish mining strategy.

Regardless of whether this will lead to the monetary gain or not, we emphasize that the selfish mining strategy could lead to the abnormal high probability of consecutively discovering two blocks. In addition to that, our result also shows that both mining pools with high computing power and those with lower computing power could conduct selfish mining strategy. This finding is against the previous finding that only mining pools with at least 25% computing power would have the incentive to perform selfish mining strategy [6]. This is might because although the analytical model shows that selfish miners with less than 25% computing power is non-profitable, in reality, people have bounded rationality (or sometimes they are even risk seeking) and cannot estimate the expected return of selfish mining strategy. Besides, those mining addresses with low revenue share but high MSB value could be used by selfish miners to hide their strategic behavior.

Given the fact that secret mining cartels may cause certain threats to the security of blockchain-based systems, we have extended our model to pair of pools in order to detect mining cartels. We have found that the mining cartels exist in each system. We note that the existence of mining cartels has been ignored in many previous studies.

There are still some limitations in our work: We have proposed that the selfish mining attack and forming mining cartels are two possible reasons of the abnormal high continuously success rate. There might be other explanations (like finite diffusion times). Our next step is to extend our methods on identifying other strategic mining behaviors [21], for instance cheating by one-time use addresses.

REFERENCES

[1] P. Tasca and C. J. Tessone, "A taxonomy of blockchain technologies: Principles of identification and classification," *Ledger*, vol. 4, no. 0, 2019.
[2] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008.
[3] G. O. Karame, E. Androulaki, and S. Capkun, "Double-spending fast payments in bitcoin," in *Proceedings of the 2012 ACM conference on Computer and communications security*, pp. 906–917, ACM, 2012.
[4] M. Apostolaki, A. Zohar, and L. Vanbever, "Hijacking bitcoin: Routing attacks on cryptocurrencies," in *2017 IEEE Symposium on Security and Privacy (SP)*, pp. 375–392, IEEE, 2017.
[5] S. Bag, S. Ruj, and K. Sakurai, "Bitcoin block withholding attack: Analysis and mitigation," *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 8, pp. 1967–1978, 2016.
[6] I. Eyal and E. G. Sirer, "Majority is not enough: Bitcoin mining is vulnerable," in *International Conference on Financial Cryptography and Data Security*, pp. 436–454, Springer, 2014.
[7] K. Nayak, S. Kumar, A. Miller, and E. Shi, "Stubborn mining: Generalizing selfish mining and combining with an eclipse attack," in *2016 IEEE European Symposium on Security and Privacy (EuroS&P)*, pp. 305–320, IEEE, 2016.
[8] H. Liu, N. Ruan, R. Du, and W. Jia, "On the strategy and behavior of bitcoin mining with n-attackers," in *Proceedings of the 2018 on Asia Conference on Computer and Communications Security*, pp. 357–368, ACM, 2018.
[9] A. Sapirshtein, Y. Sompolinsky, and A. Zohar, "Optimal selfish mining strategies in bitcoin," in *International Conference on Financial Cryptography and Data Security*, pp. 515–532, Springer, 2016.
[10] Q. Bai, X. Zhou, X. Wang, Y. Xu, X. Wang, and Q. Kong, "A deep dive into blockchain selfish mining," in *ICC 2019-2019 IEEE International Conference on Communications (ICC)*, pp. 1–6, IEEE, 2019.
[11] S. Solat and M. Potop-Butucaru, "Brief announcement: Zeroblock: Timestamp-free prevention of block-withholding attack in bitcoin," in *International Symposium on Stabilization, Safety, and Security of Distributed Systems*, pp. 356–360, Springer, 2017.
[12] R. Zhang and B. Preneel, "Publish or perish: A backward-compatible defense against selfish mining in bitcoin," in *Cryptographers' Track at the RSA Conference*, pp. 277–292, Springer, 2017.
[13] C. S. Wright and S. Savanah, "The fallacy of the selfish miner in bitcoin: An economic critique," 2017.
[14] J. Bonneau, A. Miller, J. Clark, A. Narayanan, J. A. Kroll, and E. W. Felten, "Sok: Research perspectives and challenges for bitcoin and cryptocurrencies," in *2015 IEEE Symposium on Security and Privacy*, pp. 104–121, IEEE, 2015.
[15] H. Dalton, "The measurement of the inequality of incomes," *The Economic Journal*, vol. 30, no. 119, pp. 348–361, 1920.
[16] J. Morgan, "The anatomy of income distribution," *The review of economics and statistics*, pp. 270–283, 1962.
[17] H. Theil, "Statistical decomposition analysis; with applications in the social and administrative sciences," tech. rep., 1972.
[18] C. Decker and R. Wattenhofer, "Information propagation in the bitcoin network," in *IEEE P2P 2013 Proceedings*, pp. 1–10, IEEE, 2013.
[19] K. Yu, M. Arifuzzaman, Z. Wen, D. Zhang, and T. Sato, "A key management scheme for secure communications of information centric advanced metering infrastructure in smart grid," *IEEE Transactions on Instrumentation and Measurement*, vol. 64, no. 8, pp. 2072–2085, 2015.
[20] C. Yang, L. Tan, N. Shi, B. Xu, Y. Cao, and K. Yu, "Authprivacychain: A blockchain-based access control framework with privacy protection in cloud," *IEEE Access*, vol. 8, pp. 70604–70615, 2020.
[21] Z. Guo, Y. Shen, A. K. Bashir, M. Imran, N. Kumar, D. Zhang, and K. Yu, "Robust spammer detection using collaborative neural network in internet of thing applications," *IEEE Internet of Things Journal*, pp. 1–1, 2020.